HIPAA Privacy Policy Updates

2008 Data Protection Seminar
TMA Privacy Office

Purpose

- Provide information about the Health Information Portability and Accountability Act (HIPAA) privacy policy updates which impact how TRICARE Management Activity (TMA) staff protect health information

Objectives

- This presentation will:
  - Describe the proposed changes to the Department of Defense (DoD) Health Information Privacy Regulation, DoD 6025.18-R
  - Describe elements of the two new TMA policies: (1) TMA Workforce Training Policy Pursuant to the DoD Privacy Act Regulations and DoD Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations and (2) Sanction Policy for Privacy and Security Violations
  - Describe the current status of compliance and enforcement activities by the Secretary, Department of Health and Human Services (DHHS)

Introduction

- Data protection is everyone’s business
- There are significant privacy consequences regarding the protection of Personally Identifiable Information (PII) and Protected Health Information (PHI) which impact our daily work
- It is important that we be well-versed in the regulatory guidance and organizational policies which impact these protections

Background

- DoD 6025.18-R recently reviewed by TMA Privacy Office staff
- Proposed changes were reviewed by TMA Privacy Officer, Office of General Counsel and Health Information Privacy and Security Compliance Committee (HIPSCC) voting members
- 93 recommended changes:
  - Majority are “minor” changes, including grammar, format, spelling, etc.
  - Substantive changes include new language or revisions to existing language

Proposed Chances to DoD 6025.18-R

Sanctions

- Added language that sanctions shall reasonably relate to the severity and nature of the failure or misconduct
- Added a reference to Public Law 108-136 for application of sanctions to civilian employees

Proposed Chances to DoD 6025.18-R

Complaints

- Added a new implementation specification- Submission of Complaints
- Individual complaints within the Military Health System (MHS) may be directed to the covered entity's Privacy Officer/Official
- Added individual's right to address complaints with TMA Privacy Officer or DHHS
- Additional instructions on filing complaints can be found on the TMA Privacy Office and DHHS websites

Proposed Chances to DoD 6025.18-R

Training

- Additional training requirements:
  - Annual refresher training for all members of workforce
  - Armed Forces Reserve Medical personnel upon mobilization or assignment for operational support to an active duty MTF, Inactive Duty Training (IDT) or Annual Training
  - Requires that training developed by TMA be used throughout the MHS

Proposed Chances to DoD 6025.18-R

FOIA and Deceased Individuals

- FOIA generally does not protect records and privacy of deceased individuals but it does offer an exemption
- Added language which discusses implications of FOIA Exemption #6
  - "If disclosure of deceased person's PHI may rekindle grief, anguish, pain, embarrassment or disrupt peace of mind of surviving family members, the covered entity must balance surviving family member's privacy against the public right to know to determine if disclosure of a deceased person's PHI is in the public interest"

Proposed Chances to DoD 6025.18-R

FOIA and Deceased Individuals (continued)

- Added language which discusses implication of FOIA Exemption #7
  - Prevents disclosure of PHI of deceased for law enforcement purposes if disclosure can **reasonably** be expected to result in an unwarranted invasion of the personal privacy of surviving family members

Verification of Identity and Authority

- Added a standard for Verification of Identity and Authority prior to disclosure of PHI
- Added implementation specifications on conditions of disclosure (i.e. public officials requests, individual requests, etc.)
- **Verification of identity of a public official**: agency ID badge or other official credentials if in person; written requests must be on appropriate agency letterhead
- **Verification of identity of an individual**: military ID card, driver's license, employment ID badge, passport, or other government issued identification

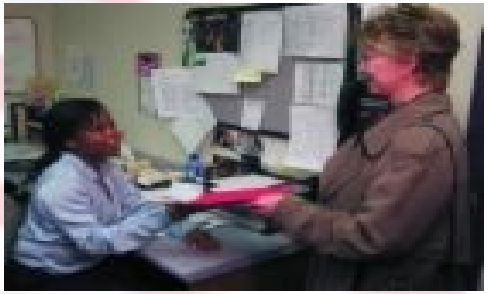
Verification of Identity and Authority (continued)

- Authority of Public Officials can be verified by written or oral statement
- If request is made for a legal process, then legal authority can be established through warrant, subpoena, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal
- Verification requirements permit exercise of professional judgment

Proposed Chances to DoD 6025.18-R

Restrictions and Authorizations

- Added language regarding use of two forms:
  - DD Form 2871, “Request to Restrict Medical or Dental Information”
  - DD Form 2870, “Authorization Form”
  - Oral and written requests for restriction may be documented on DD Form 2871
  - Forms available on TMA Privacy Office website



TMA Workforce Training Policy

Purpose

- Ensure that all TMA workforce members who have access to PII and/or PHI are properly trained
- Requirement under DoD 5400.11-R, “ Department of Defense Privacy Program,” May 14, 2007, and DoD 6025.18-R, “Department of Defense Health Information Privacy Regulation, January 2003

Applicability and Scope

- The TMA Sanctions policy applies to:
  - TMA Directorates
  - TROs
  - TAOs and all TMA components
  - Workforce members including military, government civilians, and TRICARE contractors, when required by contract

Applicability and Scope

- The TMA Workforce Training policy applies to:
  - TMA Directorates
  - TRICARE Regional Offices (TROs)
  - TRICARE Area Offices (TAOs) and all TMA components
  - Workforce members including military, government civilians and TRICARE contractors, when required by contract

Policy Highlights

- **Annual Training**: TMA workforce members required to participate in annual privacy and security related training, to include information assurance training; must sign acknowledgement
- **Refresher Training**: TMA workforce members required to complete annual privacy and security refresher training
- Newly assigned staff must complete required training and sign an acknowledgement/certification of training in order to gain access to TMA systems
- Delivery method: TMA Learning Management System (currently MHS Learn) or other automated options

TMA Sanctions Policy for Privacy and Security Violations

Purpose

- Outline how sanctions should be determined and applied against TMA workforce members who fail to follow appropriate standards for safeguarding PII/PHI

Policy Highlights

- Director, TMA Privacy Office coordinates with TMA Human Resource Department and Office of General Counsel in determining specific sanctions
- Sanctions are based on “severity and circumstances” of the violations
- Type and severity of sanctions imposed and categories of “violation” are at the discretion of TMA

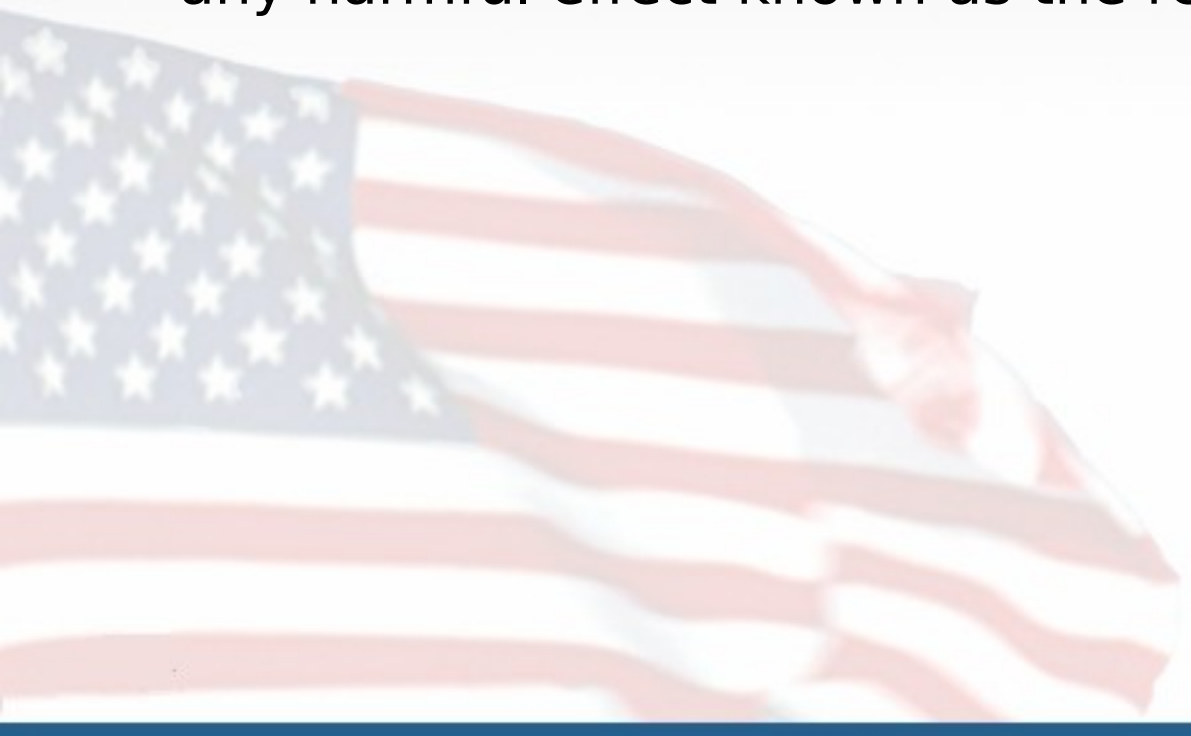
Policy Highlights (continued)

- Sanctions against military personnel may include action under the Uniform Code of Military Justice (UCMJ)
- Sanctions against civilian employees governed by provisions of Chapter 75 of Title 5, United States Code (Adverse Actions)
- Sanctions against contractor personnel governed by applicable procurement regulations and Business Associate Agreements (BAAs) and/or other agreements when required by contract

TMA Sanctions Policy

Responsibilities

- Director, Human Resources Division documents sanctions and maintains written or electronic records on military and civilian employees only
- Director, TMA Privacy Office assigns tasks to mitigate any harmful effect known as the result of a violation



Exception

- Policy does not apply to a TMA workforce member if his/her actions meet conditions outlined in DoD 6025.18-R, “Department of Defense Health Information Privacy Regulation” regarding whistleblowers and workforce member crime victims

HHS Compliance and Enforcement

HHS Compliance and Enforcement

General Information

- DHHS Final Enforcement Rule published 2/16/06
- Office for Civil Rights (OCR) responsible for Privacy Rule enforcement
- Center for Medicare and Medicaid Services (CMS) responsible for Security Rule enforcement
- Department of Justice (DoJ) investigates criminal allegations

Civil Money and Criminal Penalties

- Civil money penalties: No more than $100 for each violation; no more than $25,000 for identical violations during a calendar year (1 Jan -31 Dec)
- Criminal penalties: Up to $50,000 in fines; imprisonment for up to 1 year

Complaints

- Filed with DHHS within 180 days of when person knew or should have known about alleged violation
- Time limit may be waived if individual demonstrates "good cause"
- Statistical Breakout of Complaints (CY 2003-2007)
  - Received 32,595 total complaints; 25,536 resolved (78%); 6,418 corrective action taken (25%); 2,690 no violation (11%)
- Majority of investigated cases closed with corrective action pertain to impermissible uses and disclosures, access, safeguards, and minimum necessary issues

Summary

- You now can:
  - Describe the proposed changes to the Department of Defense (DoD) Health Information Privacy Regulation, DoD 6025.18-R
  - Describe elements of the two new TMA policies: (1) TMA Workforce Training Policy Pursuant to the DoD Privacy Act Regulations and DoD Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations and (2) Sanction Policy for Privacy and Security Violations
  - Describe the current status of compliance and enforcement information from Secretary, Department of Health and Human Services (DHHS)

Case Scenarios

Issues and Management

- Notify TMA Privacy Officer (PO), who then coordinates with the Human Resources Department and Office of General Counsel to determine specific sanctions imposed based on the “severity and circumstances” of the violation
- Guidance for sanctions for civilian employees should be consistent with provisions of Chapter 75 of Title 5 (Adverse Actions) and Public Law 108-136.
- Director, Human Resources will document the sanctions imposed and maintain appropriate documentation
- TMA Privacy Officer will assign and monitor any tasks necessary to mitigate harmful effects of the violation

Case Scenario # 2 TMA Workforce Training Policy

Issues and Management

- Ensure LCDR Healthy completes all initial required training referenced in the TMA Workforce Training Policy
- Ensure LCDR Healthy also completes annual refresher training
- You are responsible for ensuring that follow on annual certification (awareness of responsibilities) shall be signed at the completion of annual refresher training
- Ensure that LCDR Healthy knows how to access the required training
- LCDR Healthy will need to complete HIPAA Privacy and Privacy Act training (role based), Security Awareness training, and required Information Assurance Training (initial and refresher)
- LCDR Healthy will sign a certification to acknowledge awareness of his responsibilities for the protection of PII/PHI before he can obtain access to the TMA network